Práctica 6 - Capa de Aplicación

Noviembre, 2020

1) ¿Cuáles son las funciones de la capa de aplicación? Compare funcionalidades entre modelo OSI y TCP/IP.
2) Describa el paradigma cliente/servidor y P2P.
3) ¿Qué es un User-Agent? Nombre algunos que conozca e indique qué protocolo de aplicación soportan?

DNS

4) ¿Cuál es el objetivo del protocolo DNS? ¿Cómo funciona? ¿Es posible que Internet funcione sin este servicio?
5) ¿Qué protocolo de la capa de transporte utiliza? ¿Qué puertos?
6) ¿Qué es un root-server? ¿Qué son los TLD? Diferencias entre gTLD y ccTLD? Indique 3 ejemplos de c/u. Cómo se acceden y que tipo de consultas se les hacen.
7) 7. ¿Qué se el *resolver*? ¿Cómo se configura en Linux y en Windows? ¿Qué tipos de resolvers hay?
8) ¿Cuándo una respuesta es autoritativa?
9) Explique las diferencias entre una consulta iterativa y una recursiva
10) Indique un posible orden de los nombres de servidores consultados desde la raíz para resolver el nombre www.info.unlp.edu.ar
11) Describa la relación de los servidores primario/secundario, determine cuales son los servidores de DNS autoritativos de los dominios .com , .ar , .yahoo.com , edu.ar e indique cuál es el primario.

12) Explique para que se usan cada uno de los siguientes tipos de registros de DNS:
    - SOA
    - A
    - AAAA
    - CNAME
    - PTR
    - NS
    - MX

13) En una caché DNS, ¿qué problemas conllevaría cambiar la dirección IP de, por ejemplo, el nombre de servidor de mail? ¿Cómo podría ser minimizado?

14) Mediante algunos de los comandos de DNS (dig, nslookup o host), contestar las siguientes preguntas:

a) ¿Cuántos servidores raíces (ROOT-Servers) hay? Indique las direcciones IP del servidor “B” y “J”.

b) ¿Cuántos servidores de correo aceptan mails en gmail.com? ¿Qué tipo de consulta es enviada para obtener la respuesta?

c) ¿Cuál es el servidor SMTP principal de gmail.com? ¿En base a qué información se puede determinar esto? ¿Utiliza IPv6 Gmail ?

d) Realice esta misma consulta contra hotmail.com. Nota alguna diferencia en las respuestas

e) ¿Cuántos servidores de nombre existen para google.com? ¿Siempre se obtiene la misma respuesta?

f) ¿Cuál es el nombre asociado a la dirección IP 163.10.0.145? ¿Qué tipo de consulta DNS es enviada para obtener la respuesta?

15) De acuerdo a lo obtenido en la figura 1, responder:

```
; <<>> DiG 9.8.5-P1 <<>> mx unlp.edu.ar
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61675
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 0

;; QUESTION SECTION:
;unlp.edu.ar.            IN    MX

;; ANSWER SECTION:
unlp.edu.ar.            19124  IN    MX    20 anubis.unlp.edu.ar.
unlp.edu.ar.            19124  IN    MX    10 unlp.unlp.edu.ar.

;; AUTHORITY SECTION:
unlp.edu.ar.            86399  IN    NS    unlp.unlp.edu.ar.
unlp.edu.ar.            86399  IN    NS    anubis.unlp.edu.ar.
unlp.edu.ar.            86399  IN    NS    ns1.riu.edu.ar.

;; Query time: 6 msec
;; SERVER: 192.168.2.1#53(192.168.2.1)
;; WHEN: Thu Sep 19 10:45:55 ART 2013
;; MSG SIZE rcvd: 123
```

a) ¿Cuántos servidores de correo hay disponibles? ¿Cuál es el servidor primario?
b) ¿Es autoritativa la respuesta? Justifique
c) Si quisiese que la respuesta fuese autoritativa, ¿a qué servidor debería realizarle la consulta?

16) Observando la captura: **`dns1.pcap`**, conteste:
    a) ¿Qué nombre de dominio se está consultando? ¿Qué tipo de registro se solicita?
    b) ¿Qué tipo de consulta se realiza: recursiva o iterativa? ¿Cómo puede saber esto?
    c) ¿Que obtiene el cliente en el segundo mensaje? ¿A qué servidor realiza la siguiente consulta?

HTTP

17) ¿Qué protocolo de la capa de transporte utiliza? ¿Qué puertos?
18) ¿Cuáles son las principales diferencias entre HTTP 1.0 y HTTP 1.1?
19) ¿Qué cambios hace HTTP 2?
20) ¿Por qué HTTP es un protocolo sin estados (stateless)?
21) Si una página web contiene un archivo base HTML y 4 imágenes. ¿Cuántas conexiones TCP son necesarias en HTTP 1.0 para obtener toda la página? ¿Y en HTTP 1.1?
22) Explique las diferencias entre los métodos GET, POST y PUT.
23) De acuerdo a lo obtenido en la figura 2, responder:

```
user1@apolo:~$ telnet www.unlp.edu.ar 80
Trying 163.10.0.145...
Connected to www.unlp.edu.ar.
Escape character is '^]'.
HEAD / HTTP1.1

HTTP/1.1 200 OK
Server: Apache
X-Powered-By: PHP/5.3.3-7+squeeze14
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
Date: Sun, 17 Nov 2013 21:21:31 GMT
X-Varnish: 738122746 738122076
Age: 28
Via: 1.1 varnish
Connection: close
X-Cache: HIT
```

a) ¿Qué método de acceso a la página se está utilizando? ¿Para qué sirve este método?¿Cuál debería usar si quiero acceder a toda la página?
b) ¿Qué versión del protocolo HTTP se utilizó en la consulta? ¿Cuál en la respuesta?
c) ¿Es correcta la respuesta del servidor? ¿Por qué?
d) ¿Cuántas cabeceras hay en la respuesta?
e) ¿Qué servidor se está ejecutando?
f) ¿Qué significa la X- en las cabeceras?

24) Observando la captura:h **`http_capture_1.pcap`**, responder:

En la línea 4 de la captura:

¿Qué versión de HTTP se utilizó?
¿A qué servidor se le envía la solicitud? ¿Qué recurso se está solicitando?
¿Qué lenguaje se acepta?
¿Qué charset se aceptan? ¿Cuál se prefiere? ¿Por qué?
¿Para qué se utiliza el header Connection: keep-alive?

En la línea 6 de la captura:

¿Es exitosa la respuesta? ¿Por qué?
¿Qué servidor envía la respuesta? ¿Qué versión del protocolo se está utilizando?
¿Para qué sirve el Header ETAG?
¿La conexión es persistente? ¿Por qué?

En la línea 8 de la captura:

¿Para qué se utiliza la cabecera If-Modified-Since? ¿Qué respuesta se obtiene?
¿Qué funcionalidad tiene la cabecera Pragma: no-cache? ¿Se la sigue utilizando? ¿Qué cabecera la reemplaza?
¿Qué finalidad tiene la cabecera If-None-Match?

25) Suponga un cliente HTTP 1.0 se conecta a un servidor HTTP 1.1 y realiza las siguientes peticiones: http://www.http11.com.ar/, http://www.http11.com.ar/index.html, http://www.http11.com.ar/home.html dentro de un una ventana de tiempo de 1 minuto.

a) ¿Cuántas conexiones TCP se utilizarían si ninguna de las páginas contiene referencias a otros objetos?
b) ¿Cuántas conexiones TCP se utilizarán si home.html tiene los TAGs HTML:
<IMG SRC="dd.jpg"> y <A HREF="otro.html">
c) ¿Qué sucedería si el cliente y el servidor soportaran ambos HTTP 1.1 ?
d) Responda la misma pregunta que la anterior suponiendo que entre la primera y la segunda petición la máquina donde ejecuta el cliente se reinicia. (Justifique todas sus respuestas).

26) ¿Cuál es la funcionalidad de las cookies?

E-MAIL (SMTP, POP, IMAP)

27) ¿Qué protocolos se utilizan para el envío y la recepción de mails? ¿Qué protocolos de la capa de transporte utilizan y qué puertos?
28) ¿Cuáles son las diferencias entre SMTP y ESMTP?
29) ¿Cuáles son las diferencias entre POP e IMAP? ¿Cuál supone que utilizan gmail o hotmail?
30) Envíe un email utilizando los comandos SMTP vía un terminal virtual de telnet a su cuenta. Averigüe primero mediante comandos la resolución de registros de DNS y luego realice la conexión usando el comando telnet server-MX 25
31) Repita el procedimiento cambiando los encabezados, por ejemplo From:.
32) ¿Para qué sirve la extensión MIME?
33) Contestar las siguientes preguntas observando el archivo: **`mail_1.pdf`**:
    a) ¿Para qué sirve la cabecera Return-Path?
    b) ¿Desde qué dirección IP se envió el mail?
    c) ¿Qué User-Agent se usó para enviar el mensaje?
    d) ¿Qué versión de MIME se está utilizando?
    e) ¿Qué tipo de información y codificación se envía en el mail?
    f) ¿Para qué se usa el campo boundary=‘‘=1rn50g4mnglf’’?
    g) ¿Cuántos attachments (adjuntos) se enviaron?

FTP

34) ¿Por qué FTP utiliza dos puertos?
35) ¿Cuáles son las diferencias entre FTP Activo y FTP Pasivo?
36) ¿FTP cifra las sesiones? ¿Qué debería usar para lograr est